INTERNATIONAL STANDARD ISO/IEC 15946-1:2008
TECHNICAL CORRIGENDUM 1

Published 2009-02-15

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Security techniques — Cryptographic techniques based on elliptic curves —

Part 1: General

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Techniques de sécurité — Techniques cryptographiques basées sur les courbes elliptiques —

Partie 1: Généralités

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 15946-1:2008 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page iii, Contents

Add the following entry above the entry for Bibliography:

"**Annex D** (informative) **Summary of coordinates** ..... **28**"

Page 1, 2.2

Convert the existing note to NOTE 1 and add the following new note:

"NOTE 2 A definition of a cubic curve is given in bibliography item [16]."

Page 30, Bibliography

Delete item [3].

ICS 35.040 **Ref. No. ISO/IEC 15946-1:2008/Cor.1:2009(E)**

© ISO/IEC 2009 – All rights reserved

Published in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale